## REMARKS

Claims 1-12 and 23-27 are pending. Claims 1-12, 23, and 27 stand rejected under the judicially created doctrine of obviousness-type double patenting over U.S. Patent No. 5,870,723 to Pare, Jr. et al. in view of U.S. Patent No. 6,269,348 to Pare, Jr. et al. Claims 1-12 and 23-27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,070,141 to Houvener et al. in view of U.S. Patent No. 5,291,560 to Daugman.

Reconsideration is requested. No new matter is added. Terminal disclaimers will be filed to overcome the obviousness-type double patenting rejections of claims 1-12, 23, and 27 once the claims are allowed over the prior art. Claim 1 is amended to move a limitation into new dependent claim 28, which is added. Claim 12 is amended to correct a typographical error. The rejections are traversed. Claims 1-12 and 23-28 remain in the case for consideration.

## REJECTION OF CLAIMS 1-12, 23, AND 27 AS BEING OBVIOUSNESS-TYPE DOUBLE PATENTED OVER U.S. PATENT NO. 5,870,723

The Examiner indicated that the Response to the Office Action dated January 18, 2002, referred to an enclosed terminal disclaimer. The Applicant acknowledges that no terminal disclaimer was actually included with that Response. As indicated in the Response to the Office Action dated October 23, 2002, a terminal disclaimer will be filed once the claims are allowed over the prior art.

## REJECTION UNDER 35 U.S.C. § 103(a)

Referring to claim 1, the invention is directed toward a method for performing tokenless authorization of commercial transactions. A user registers a biometric sample and a financial account. A seller also registers a financial account. The seller proposes a commercial transaction. The proposed commercial transaction, including user personal identification information, comprising at least a bid biometric sample, is transmitted to a computer system. The user is identified by comparing the bid biometric sample with registration biometric samples. The user's financial account is debited and the seller's financial account is credited. The commercial transaction is conducted without the user using smart cards or swipe cards.

In contrast, Houvener teaches a system for assessing the quality of an identification. In Houvener, the user presents a card, such as a credit card. The clerk inputs the account number to the system either by reading the account number electronically off the card or by manually inputting the account number. The account number is forwarded to an identification database. The account number is found in the database, and an identification (such as a photo) is returned to the clerk. The clerk compares the identification with the user to complete the user identification, and if there is a match, the transaction is performed.

The Examiner acknowledged on page 6 of the Office Action dated June 19, 2003, that Houvener only explicitly teaches using the account number to locate the biometric data. The Examiner argued that Houvener teaches that the system can be adapted to systems in which, the Examiner asserts, the customer would not have an account number. Thus, the Examiner argues that the biometric can be input to the system, and the account number can be returned from the system.

Finally, the Examiner acknowledged on page 7 of the Office Action dated June 19, 2003, that Houvener does not teach comparing the current biometric data against a plurality of customers in the database. The Examiner cites to U.S. Patent No. 5,291,560 to Daugman as teaching comparing biometrics.

First, there is no motivation to combine Houvener and Daugman, as suggested by the Examiner. The Examiner argues that the motivation to combine the references would be to "automatically and unobtrusively identify the customer." But Houvener is concerned with verifying the earlier identification. Nowhere does Houvener suggest that, instead of biometric verification, improved identification is needed to enhance the security of the described financial transaction system. And Daugman teaches only iris identification, without tying it to any particular use, let alone executing a financial transaction.

Second, Houvener's described use for the biometric is for user *verification*, not user identification. Houvener describes a way to improve the security of an existing system. That is, the situation Houvener was addressing was the weakness inherent in credit card transactions. Before Houvener, the system operated by having the user present a credit card to the clerk. The user would sign the receipt. The clerk would then attempt to verify the user's identity, perhaps by comparing the signature on the receipt to the one on the back of the card, or by comparing some additional data provided by the user to data stored on the credit card. Houvener modified this system by having the system perform the verification without tying it to data easily accessed by parties interested in perpetrating fraud. To read Daugman as suggesting that Houvener would benefit from improving the identification process is to apply hindsight to the prior art, as Houvener was only concerned with using biometrics to verify the user's identity. Since the claims are to be analyzed for obviousness without hindsight, the Examiner's comments suggest that the claims are, in fact, non-obvious over Houvener.

Third, even if Houvener could be adapted as suggested by the Examiner (a position the Applicant disputes), the result would not be logical, and would not be the claimed invention. Houvener is a two-step process. In the first step, the user is identified using an account number. In the second step, the user's identity is verified using biometrics. Only after these two steps are complete is the transaction performed, using the account number originally provided.

In contrast, the invention is a one-step process. Using the user's biometric, the user is identified, and his account number retrieved. The transaction is then performed using the retrieved account number.

There are at least two reasons why Houvener cannot be adapted as suggested by the Examiner. First, the Examiner argues that there are situations in which the customer would not have an account number, and therefore could not enter an account number. But if there is no "account number," then the only data stored by the system are the biometric data: there would be no second identification unit returned by the system. As Houvener explicitly teaches that there are two identification units in the information database (see column 3, lines 15-19: the summary of the invention), Houvener calls for the user to register some information other than the biometric data.

In addition, the argument that the second identification unit might be something other than an account number, even if an accurate statement in and of itself, misses the fact that the second identification unit would still be some uniquely identifying information. For all of the system adaptations (firearm sales, food stamp reimbursement or other welfare-related uses, voting, law enforcement, health care, airline, and immigration and naturalization), there would still be some uniquely identifying number assigned to the user. In most cases, it would be a government issued identification, such as a driver's license number or other identification card; for some, it might be a number assigned to the user by the system operator. For example, firearm sales require a background check, which are performed by the government. The identification number would then be either a driver's license number or a social security number. But for health care, the number might be the patient record number assigned by the health care provider, and for airlines, the number might be a frequent flier number assigned by the airline. In all cases, there is still a unique identification number assigned to the user; that the number is not a financial account number is irrelevant, and this number, financial account number of otherwise, would be used to search the identification database.

The second problem with the Examiner's reasoning lies in the use of the second identification unit. As described in Houvener at column 3, lines 41-46, the second identification unit is used to verify the user's identity. In the described embodiment, the second identification unit is a photo of the user. Thus, after the user presents his financial account, the associated photo is retrieved, so that the clerk can compare the photo against the person physically present to confirm the user's identity. Even if the biometric data and the financial account number (that is, the two identification units) could be interchanged in terms of which is used to locate the other, the financial account cannot be used by a clerk to verify the user's identity: it is an arbitrary number assigned by some third party that has no value outside its association with the user. The clerk cannot look at the financial account number and compare it with the physical appearance of the user to verify the user's identity.

Even where the second identification unit is used to automatically verify the user's identity (that is, the clerk does not manually verify the user's identity), it still makes no sense to use the account number to verify the user's identity. The account number is just that: a number. The only relationship, direct or otherwise, between the account number and the user is the fact that the account number is assigned to the user. Thus, the account number intrinsically provides no capability for verifying a user's identity. The Examiner is asked to note that it is relatively easy for a party intent on fraud to intercept an account number. As the purpose behind Houvener's adding the verification step to the prior art transaction process is to increase security that the user performing the transaction is the proper user, the account cannot be used to improve security in verifying the user's identity, which is the stated purpose of the second identification unit of Houvener.

Another problem with the Examiner's reasoning lies in how the identification step is done in the invention versus Houvener. The Examiner suggests that, because Houvener teaches the use of an account number to find a biometric data, it would have been obvious to a person skilled in the art to reverse the roles of Houvener's first and second identification units: i.e., to use a biometric data to find an account number. But searching for an account number is very different from searching for a biometric. With account numbers, comparison is easy: numbers (and letters, which are both digital data) either match or they do not. But with biometrics (stored as a digital representation of analog data), a comparison does not return a simple "yes" or "no" answer.

There are any number of reasons why the match would not be perfect. For example, the user may be positioned differently relative to the biometric sensor than he was when the registration biometric sample was taken. Or, the user may be physically different from when the registration biometric sample was taken (e.g., if an iris pattern is used, the blood vessels in the user's eye might be inflamed). Because the process for comparing digitized versions of analog data is very different from the process for comparing digital data, the two are not interchangeable, and Houvener neither teaches nor suggests comparing analog data (biometrics) to locate an account number. Therefore, Houvener cannot teach forwarding the bid biometric sample.

In addition, even if it would be obvious to interchange the roles of the biometric data and the account number (a position the Applicant disputes), Houvener still teaches using the second identification unit to verify the user's identity. As argued earlier, an account number cannot be used to verify identity, since it provides no confirmatory information. Thus, not only is it not obvious to interchange the roles of the biometric data and the account number, but such a change would not be the same as the invention as claimed.

In addition, despite the Examiner's assertion to the contrary, Houvener neither teaches nor suggests that the roles of the biometric data and the account number can be interchanged. The Examiner's suggestion that Houvener can be adapted by interchanging the roles of biometric data and account number is contrary to the disclosure in Houvener, and one for which the Examiner has not shown any motivation. In fact, no such motivation can be presented, since, as discussed above, Houvener cannot be modified to interchange the roles of the biometric data and account number.

As stated above, Houvener was designed to enhance the security of an identification process by adding a biometric verification step to the process. But the invention performs identification without needing the addition verification step of Houvener. That the invention can perform the identification completely in one step, rather than two, is surprising, and shows that the invention is not obvious over Houvener.

Finally, Houvener teaches a system using tokens. As described, in Houvener the user presents a token, such as a credit card or a driver's license. The clerk uses the token to access the account number: e.g., by swiping the credit card. Because Houvener depends on tokens to operate, Houvener does not teach or suggest a system that operates without tokens, as claimed.

The invention as defined by claim 1 is directed toward:

> A method for tokenless authorization of commercial transactions between a user and a seller using a computer system, the method comprising the steps of:
>
> a. a user registration step, wherein the user registers with the computer system at least one registration biometric sample and at least one user financial account;
>
> b. a seller registration step, wherein the seller registers with the computer system at least one seller financial account;
>
> c. a proposal step, wherein the seller offers a proposed commercial transaction to the user, the proposed commercial transaction comprising price information;
>
> d. a transmission step, *wherein the user's personal identification information comprising at least a bid biometric sample is forwarded to the computer system*;
>
> e. a user identification step, wherein *the computer system compares the bid biometric sample with registration biometric samples for producing either a successful or failed identification of the user*; and
>
> f. a payment step, wherein a financial account of the user is debited and a financial account of the seller is credited, *wherein a commercial transaction is conducted without the user having to use any smartcards or swipe cards.*

(claim 1; italics added). As these features are not taught or suggested by Houvener or Daugman, claim 1 is patentable under 35 U.S.C. § 103(a) over Houvener in view of Daugman. Accordingly, claims 1-12 and 23-27 are allowable.

Referring to claim 11, the invention is directed toward a method for performing tokenless authorization of commercial transactions. Claim 11 adds to the method of claim 1 a user re-registration step. The Examiner argues that Houvener teaches checking incoming registration biometric samples against previously stored biometric samples. The Examiner cites to column 6, lines 52-67, and column 7, lines 38-42, for support for this assertion. But the cited portions of Houvener do not teach checking registration biometric samples against previously recorded biometric data. Instead, column 6, lines 52-67 describes how the information database stores identification quality scores. These identification quality scores identify accounts that are considered susceptible to fraud, so that clerks can be more careful before completing the transaction. And column 7, lines 38-42 describes one condition which might indicate fraud: namely, an individual registering a large number of accounts, either in a short span of time or under different names with a common address. Neither of these sections describes comparing an offered registration biometric sample with previously registered biometric samples. Further, as described above with reference to claim 1, Houvener does not describe comparing biometric samples at all, and so cannot teach or suggest checking an offered registration biometric sample against previously registered biometric samples, to guard against a user re-registering.

The invention as defined by claim 11 is directed toward:

> The method of claim 1 further comprising a user re-registration check step, wherein *the user's registration biometric samples are compared against previously designated biometric samples of certain users wherein if a match occurs, the computer system is alerted to the fact that the user has re-registered*, whereby users who perpetrate fraud on the system can be automatically identified from their biometrics alone if and when they re-register.

(claim 11; italics added). As these features are not taught or suggested by Houvener or Daugman, claim 11 is patentable under 35 U.S.C. § 103(a) over Houvener in view of Daugman. Accordingly, claim 11 is allowable.

Referring to claim 24, the invention is directed toward a method for performing tokenless authorization of commercial transactions. Claim 24 describes the transmission step of claim 1 as forwarding only the bid biometric data, and not the financial account. As described above with reference to claim 1, Houvener uses the account number to access the biometric, and the roles of the biometric data and the account number are not interchangeable. Therefore, Houvener cannot teach or suggest transmitting the biometric data without transmitting the financial account.

The invention as defined by claim 24 is directed toward:

> The method of claim 1, wherein the transmission step *forwards the bid biometric sample to the computer system in the absence of the user financial account.*

(claim 24; italics added). As these features are not taught or suggested by Houvener or Daugman, claim 24 is patentable under 35 U.S.C. § 103(a) over Houvener in view of Daugman. Accordingly, claim 24 is allowable.

For the foregoing reasons, reconsideration and allowance of claims 1-12 and 23-28 of the application as amended is solicited. The Examiner is encouraged to telephone the undersigned at (503) 222-3613 if it appears that an interview would be helpful in advancing the case.

Respectfully submitted,

MARGER JOHNSON & McCOLLOM, P.C.

Ariel S. Rogson
Reg. No. 43,054

MARGER JOHNSON & McCOLLOM, P.C.
1030 SW Morrison Street
Portland, OR 97205
503-222-3613
**Customer No. 20575**

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO:

□ COMMISSIONER OF PATENTS AND TRADEMARKS WASHINGTON D.C. 20231

☒ MAIL STOP__________
COMMISSIONER FOR PATENTS
BOX 1450
ALEXANDRIA, VA 22313-1450

□ BOX __________
COMMISSIONER FOR TRADEMARKS 2900 CRYSTAL DRIVE ARLINGTON, VA 22202-3513

ON: 18 Dec 2003